Comparative analysis of monitoring system for data networks

Ondrej Marik*
Faculty of Electrical Engineering and Informatics
University of Pardubice
Pardubice, Czech Republic
ondrej.marik@student.upce.cz

Stanislav Zitta
Faculty of Electrical Engineering and Informatics
University of Pardubice
Pardubice, Czech Republic
stanislav.zitta@student.upce.cz

***Abstract* - The document is focused on comparative analysis of monitoring systems for data networks and their subsequent application to the data network with smaller range. In the text, the author describes methodology of comparison of monitoring systems and a description of their implementation and testing. In the introduction the document deals with the theory of design patterns for deployment of monitoring systems.**

***Keywords*— monitoring systems; Cacti; Nagios; SCOM; Zabbix; comparison; testing**

I. Introduction

The first experiments with data networks have started many years ago. Since then the data network branch run through a huge technical revolution and society is dependent on it and for service providers is very important their maximum availability and continuous monitoring. This fact was the main motivation for a process of comparative analysis of monitoring systems which would allow the deployment of the best-fitting system for data network of local service provider.

The concept of data networks is in the document understood as a digital packet network. From the geographic range point of view we are talking about LAN, MAN and WAN networks.

The main aim of this document is to introduce problematic of network monitoring systems to reader and acquaint him with the methodology of the tests. In first part the author explains theory of monitoring systems and describes design patterns for its implementation which is very important for decision before implementation. The second part describes results of our research which is methodology for comparing and testing of monitoring systems. The last part of document is devoted to practical application of methodology in real case.

II. Types and topology of monitoring systems

The monitoring system could be define as an element which is implemented to a target network. It also periodically checks an availability and state of each nodes and links. In the case that there any problems or that some elements are not available it automatically notify the responsible person. In some cases it is possible to actively manage the network using the monitoring system. We can also define the ways which would be used in a case that the critical node is unavailable. But it depends on a type of monitoring system which was used – in general we divide them into three types. Monitoring systems can be used as an app on a server (a case of compared systems) or as an individual device.

A. Categories of monitoring systems

1) Basic monitoring systems

Basic monitoring systems typically works with protocol ICMP. These systems periodically checks only a state of element in view and they are able to provide an information about its availableness only on available/unavailable level or they possibly add an information about time response. This type of monitoring system is suitable only for smaller LAN networks or for networks which are not able to provide more information about a device in view.

2) Advanced monitoring systems

This type of monitoring typically works with more protocols as SNMP, CDP, SSH and so on. This fact allows systems to watch practically all information about devices in network as state of running services, utilization of system resources, actual data flow and so on. With servers those systems typically use local running agents which help to accumulate data which are unavailable through network´s protocol.

3) Proactive monitoring systems

Proactive monitoring systems are more or less advanced monitoring system that can manage networks devices. These systems allows to administrator implement automated script which react on predefined events and are suitable for highly automated environment such as datacentres, extensive networks, highly available clusters and so on.

B. Architecture of monitoring systems

Despite the fact that each data network is essentially unique there is a general idea of commonly applied data network architecture with respect to robustness, speed and reliability of data transmission. This architecture is best characterized and describes by Cisco Company and its called Enterprise Campus 3.0 [1]. The principle of this architecture is a three-tier hierarchical network with core, distribution and access layers which allows and facilitates networks future growth and

978-1-4799-3824-7/14/$31.00 ©2014 IEEE

significantly assists to easier routing, addressing and autonomy of the individual components and blocks of the network.

From the perspective of monitoring systems appears to be one of the most fundamental questions their location in monitored network. According to the author´s opinion the logical place for its location is the core layer which should ensure maximum availability and at the same time allow to the monitoring systems an access to all elements across network layers.

When you use a monitoring system you must take into account the size of the monitored network and according to it you must choose suitable architecture. Generally speaking, nowadays we use two monitoring systems architecture – centralized and federated.

1) Centralized monitoring system

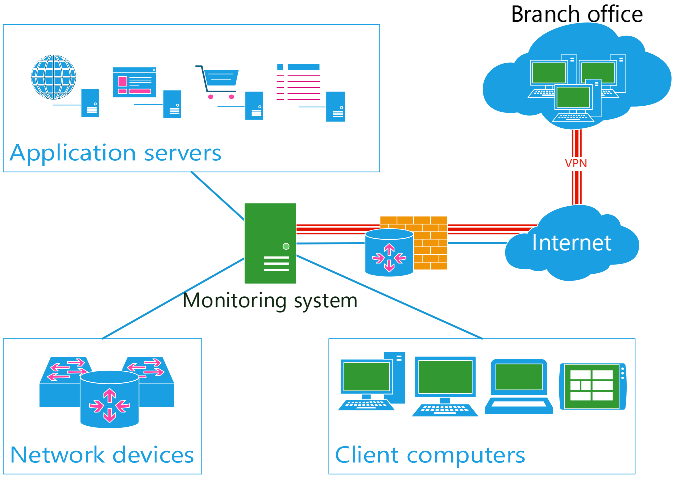

Figure 1 – The architecture of centralized monitoring system

The basic architecture and deployment of the monitoring system suitable especially for smaller networks without external branches. The monitoring system is used there only with one server which monitors the entire network. If it is necessary to monitor also the external branch, site-to-site VPN is used in most cases.

If this architecture is used, it is extremely important to choose an appropriate location of monitoring system. Logically is the best place for its connection at the centre of the network (core of the network). The problem is that if you have only on server it is impossible to get its accurate identification in case of failure for example if we connect the network in edge router.

The advantage of this architecture is simplicity and speed of implementation. The riskiest and the most challenging point of its implementation is clearly the location concept of monitoring system.

2) Federative monitoring system

This architecture is based on segmentation of monitored network to smaller parts which are monitored by individual monitoring system. These smaller servers then report entire information about the network from their point of view to the central monitoring server. The central monitoring then on the basis of the information from branch systems can quiet accurately reports the affected segment of the network. In case of failure of the main monitoring system is still possible to obtain data and information from the branch systems.

This type of architecture is suitable especially for extensive networks or on the other hand for providers who can use it to monitor their customers´ networks and outputs from the main monitoring system then present to their monitoring centre.

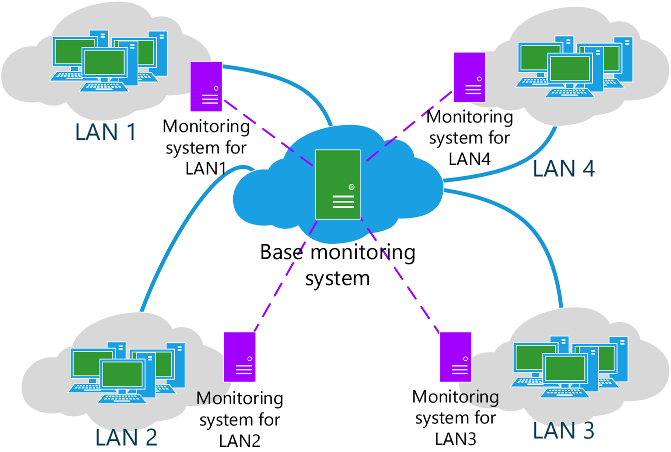
LAN 1
Monitoring system for LAN1
Monitoring system for LAN4
LAN 4
Base monitoring system
Monitoring system for LAN2
Monitoring system for LAN3
LAN 2
LAN 3

Figure 2 – The architecture of federated monitoring system

C. Monitoring mechanisms

Monitoring systems for gathering information from the monitored devices use three methods. The first one is checking of devices by using standard protocols such as ICMP, TCP, SNMP and so on. This way of checking in most cases does not require any large interventions to configuration from the monitoring device except allowing exceptions in the firewall. It is also a universal method of obtaining information regardless of makers and the type of device. The disadvantage is a certain generalization and unavailability of some specialized functions.

The second option is using SNMP notification called SNMP trap. Opposite the first option there is no periodical checking from the side of monitoring system but monitored element in case that something happened (error, port failure, RAM is full, etc.) will send a report to monitoring system which then do next action based on the information it got. This way of checking is in most cases combine with periodical checking. More information about SNMP can be found in [2].

The third option how monitoring system obtain data is using of special agent for monitored device. The agent works at the target system as an app and it communicates with monitoring system on client-server principal. The advantage is that you must not use special network protocol because the data are mostly transmitted by TCP/IP. The main benefit is a possibility to obtain detail information about monitored system and in case of proactive monitoring system there is also possibility manage the monitored station. Servers are typically monitored using this way.

III. Methodology of Testing Monitoring Systems

If you want to objectively test and compare chosen systems, it is necessary to establish assessing criteria and methods for evaluating data. For the purposes of this paper the author decided to establish a separate ranking for each assessing criterion and in the given case the best system evaluate three points. Other monitoring systems then always got one point less than the system before them. In case that there are more systems on the same position in any ranking, all of them will get maximum points.

This rigged evaluation should be conclusive enough to be possible with its help choose the most appropriate software. The methodology described in next chapters, can be used for comparing pre select systems. In real world application, whole process should consist from several steps: defining requirements, market research for potential fitting systems, methodology application, implementing winner. The possible extension of the methodology can be implementation of weight systems. With it we can prefer parameters important for us. For example if money is not problem, we probably won't that much prefer low cost solution.

A. The assessing criteria

1) The price

At the moment when we will decide about which monitoring system should be used will be its price always one of the most fundamental criterion. Unfortunately it is the price that is too overrated and the vast majority of companies cannot properly analyse this parameter. The price should be always analyse proportionally to what the system will bring us and where it will save our labour costs or streamline processes.

For the purposes of this paper is very difficult to evaluate these benefits, so I decided to compare the systems only by simple sorting.

2) System requirements

The criterion which evaluates minimal requirements for starting the system both in terms of load and also of supporting applications. The parameters for evaluation of the criterion were taken from the documentation for individual systems.

3) User interface

Probably the least predicative criterion. It is mainly because of the fact that the look and work with users interface is so subjective that it is practically impossible to obtain an objective evaluation.

Despite, the author has tried to evaluate the system from this point of view and especially from the perspective of network visualization, displaying the output graphs and the whole user comfort.

4) Difficulty of implementation

The criterion which evaluates the difficulty of installation and basic configuration of monitoring system. During the evaluating the attention was focused especially on the time which is necessary for deployment of the system, quality of documentation that describes the whole process and the time and expertise difficulty for entering monitored guests.

5) The performance on the network card

The evaluation of network traffic which is generated by monitoring system. The measurement was carried out for 24 hours. During the time data were gathering by Wireshark program which saves entire communication on the individual network card connected to monitored network. To prevent unwanted communication each monitoring system was used on dedicated virtual server with two network cards. The first one with access to the internet outside the monitored network and with default gateway. The second one was connected to the monitored network and had set only one fixed IP address without a default gateway.

Then the measurement itself was launched on the card connected to tested network and data collection was during the normal work day so it should reflect normal network traffic.

The measurement run currently in all systems, so the data were obtain under the same conditions. It means that the testing objectivity was ensured in this criterion.

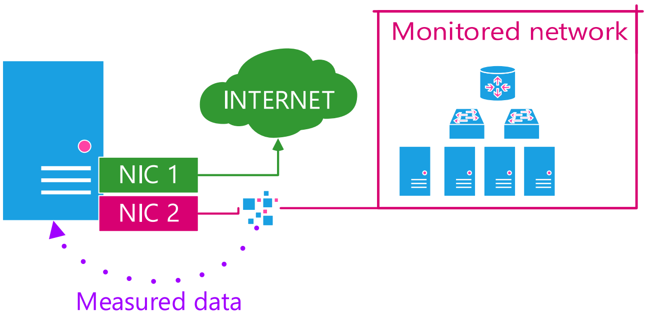

Figure 3 – The scheme of measuring the load on the network card

6) Speed of response to the failure

The criterion which evaluates the system´s ability to response to the failure of any element in the network. The original idea of this criterion was evaluation of the response time of the system. However, during testing it was found that this method of evaluation would not be sufficiently objective because most of tested monitoring systems allow you to set the interval for checking the network and some of the system even require this value in process of adding monitored element into the system.

In this respect, it has been evaluated whether the interval can be set globally for each element separately, or not. During the evaluation we also considered a possibility of setting a minimal size of interval.

7) The ability of indetification the affected segment

The evaluation especially from the perspective of possibility to define a hierarchy of monitored network and consequence ability to identify an affected segment in case of failure. At this point is evaluated especially a possibility of constructing the dependence and relations among the network nodes and both in terms of configuration and its convenience and in terms of tracking the failure.

8) Automatic search

The function, which automatically scans the area of monitoring system and searches network nodes for tracking. The monitoring systems for this tracking use ICMP and SNMP protocols. Some of the systems then use also traceroute utility for detecting a transmission path to the found node. From the perspective of this criterion is evaluated especially quality of scan, speed and recognition of the actual network topology.

9) Methods of notification

The evaluation from the perspective of the information about situation on the network sent to the administrator. When we scoring each point given to the system is for available technology. Systems typical prefer email or SMS. Some of them also adds support for various communication networks such as Jabber and so on.

10) Additional functions

The criterion which evaluates additional functions that are not a part of the standard on all tested monitoring systems. Points are given according to the number of available functions.

11) Cooperation with other systems

It is exploring interoperability among the monitoring systems and method, if it exists, how it is possible to connect systems or how to combine them. The point is given to each monitoring system which can be integrated with other systems.

12) The depth of monitoring

It evaluates the studied system from the perspective of available information about monitored devices. As the lowest layer in the case is taken the response to ICMP echo request. For the top layer is then considered monitoring of activity of running applications.

13) The real deployment

This criterion evaluates especially personal and practical experiences from the testing traffic which was running for two months. During this time was possible to consider each monitoring system and obtain valuable experience from their use. We also managed to capture and tested situations when the realised wireless connection in the centre of the city started to repetitively behave unpredictable due to intrusions (an increase latency, link outages, data loss, etc.). The monitoring systems have been tested on all commonly arisen situations on monitored network.

IV. The testing environment

The testing of chosen monitoring systems run on smaller real network which is geographically lay-out between two cities. The distance between the cities is about 46 km and connection between them I realised by optical fibre. The purpose of the site is the mediation of internet connectivity and provision of data and hosting services.

From a technological point of view the network represented both fibre and copper transmission media and wireless links. As the active elements are used Cisco switches, Mikrotik routers and for wireless links is used technology created by Ubiquity Company.

In terms of servers are represented as classic "stacked" computers and servers from IBM, HP and Cisco. From the application point of view the network includes OS Windows Server 2012 and Cent OS 6.3 including the available roles and services and database servers MS SQL 2012, Oracle 10g and MySQL.

Annex 1 shows current network structure which is simplified only to the essential elements in VLAN for network management. It was a subject for monitoring and is always ended on at the border of transmission and customer networks.

Each monitoring system was used on dedicated virtual server in visual background of Hyper-V (Hyper-V Server 2012). The performance of virtual servers was set on recommended requirements and the servers were allowed dynamic allocation of system recourses. Virtual server were running on physical server indicated in the diagram as "Bender".

In the second phase of testing of monitoring systems they were connected to the simulator for computer networks GNS. There was prepared a testing network in connection shown in annex 2. We have chosen routers Cisco C2600.The routing to the network was secured by EIGRP protocol in internal network and RIP protocol to the real network. The connection with a real network ensures Windows Server 2012 with a role of router and enable routing RIP protocol.

On this network was tested a function of automatic detection and identification of an affected segment. This move was taken mainly because the previous network was productive and was not possible to call the failures in it for purpose of this paper.

V. The evaluation of the tested system according to the methodology

To achieve the aim which was established in this work was necessary to choose a suitable candidate systems. Their selection was based primarily on the internet, searching in experts' journals and consultations with experts who had experiences with extensive networks and data centres. During the searching we considered mainly usability, references, developer base and of course representation of freely available systems as well as the commercial systems.

The result was identification of the following systems: Nagios XI, Cacti, Zabbix, Microsoft System Center 2012 Operations Manager (SCOM 2012), IBM Tivoli. Unfortunately when we try to obtain testing version we have to reject a solution from IBM which implementation is too difficult and was not possible to test it in set conditions. The author decided to continue in this work only with two freely available systems – Cacti and Zabbix and with two commercial systems – Nagios XI and SCOM 2012. All chosen systems met the author´s basic requirements to find solutions – the availability, advanced network monitoring, support of various types of devices, survivability of use.

The evaluation of the programs is based on author´s long-term testing of selected systems in the real network which was running for two months. All systems were in the testing network started up currently so it was possible to observe their behaviour differences and nuances in different situation on monitored network. During the testing there were usual circumstances and errors on standard network. The reaction of monitoring systems to the failure was properly tested mainly in wireless links which became a problem point of monitored network due to ambient intrusions.

A. The price

From price point of view are best systems Cacti and Zabbix. It is due to open source license so the cost is zero. For commercial systems is then favorable cost of Nagios XI – \$1 650 USD. The most expensive system is SCOM 2012 due to necessity of Windows Server OS which is quite expensive comparing with Linux based OS. In case of SCOM 2012 we also have to calculate with licenses for every host in view.

B. System requirements

In this field of evaluation the author have found problems with documentation of chosen systems. In case of SCOM 2012 and Cacti these requirements were not listed in deployment guides so we had to estimate it by observing real consumption of system resources on virtualization server. For Zabbix and Nagios were requirements taken from documentation.

Lower requirements has Zabbix with CPU PII 350 MHz and 256 Mb RAM. As a software support Zabbix needs Linux based OS and one of these databases – MySQL, MyISAM, InnoDB or PostgreSQL [3].

Nagios on second place had requirements two core CUP and 1-4 GB of RAM (real consumption about 800 MB), 40 GB of free space on hard disk, Linux based OS and MySQL [4].

As is written earlier, Cacti had to be measured for real system sources consumption and at the end of trial, the values stabilized on two cores CPU, 846 MB RAM and 8 GB of free hard disk space. Software requirements are MySQL, PHP 5.1++ and RRDTool 1.4+ for graph visualization. All can be run on Windows or Linux server system.

Highest requirements had SCOM 2012 where system requirements are divided on a single components of the whole system. For the purpose of this paper and evaluation the author decided to use part about management server [5] – 1GB free space, Windows Server 2008 R2 SP1+, 64-bit processors, PowerShell v2 and .NET Framework 4+. Another important requirement is MS SQL database server which has big impact on the whole system requirements of this monitoring system. After month of testing whole server needed 7 GB of RAM.

C. Difficulty of implementation

In this area was best SCOM 2012 because of its intelligent network scanning which recursively checks neighborhood of every discovered host. This feature makes deployment of SCOM very easy and comfortable.

Nagios XI finished in this area on the second place. Its installation was with documentation in mind very easy but it has only simple auto search function and we figured out small problems with it in a large range of address space. Slightly worse was the implementation of Zabbix which needs more investigation of documentation and sometimes the whole process was not intuitive. The worst from my point of view was Cacti because of templates which you need for every device you have in the network. There is general template in system but it is not sufficient for most devices.

D. User interface

There is no way how to objectively evaluate user interface because of it is all about subjective feelings. From our point of view the best user interface had SCOM 2012 because user can use web or desktop console and PowerShell command line.

Second place is for Nagios because it has only web console. On the other hand it is sufficient for regular work and it supports own dashboard, reports etc. The third was Cacti because we had sometimes problem to find items we needed. The worst user interface had Zabbix which is quite confusing in managing hosts in view.

E. The performance on the network card

This parameter is the easiest for comparing because it gives us exact numbers. The lowest average load was measured on SCOM 2012 (150.38 byte/s) followed by Zabbix with 163.57 byte/s. Bigger data growth was measured on Cacti (539 byte/s). Last and without points finished Nagios XI with 547.5 byte/s. The visualization of measured values can be found in [6].

F. Speed of response to the failure

This area was evaluated from settings point of view. Reasons were written earlier in chapter III.A.6). The best results had Zabbix where can set minimum interval a second and it can be different for every device in view. Second place is for Nagios, where interval cannot be lower for a minute. One point is for SCOM 2012 and Cacti especially for the fact that we cannot set interval individually but only as global value.

G. The ability of indetification the affected segment

The best in this discipline was SCOM 2012 because of its intelligent auto search feature followed by Nagios XI. Nagios XI had problems with detail identification because it builds tree topology and if the top of tree is unavailable to all branch it is indicated as error. One point is for Cacti and Zabbix which all nodes checks as linear address space.

H. Automatic search

During testing of this feature was clear winner SCOM 2012 with intelligent searching algorithm mentioned earlier in the document. Despite the problems with large address space it received the points for second place system Nagios XI. It is because of user-friendly wizard of the whole process. One point for ththird place is for Zabbix because of missing simple guide to go through whole process. The last finished Cacti without automatic search function (plugin available).

I. Methods of notification

The most methods contains SCOM 2012 – email, SMS, IM and scripts. The least methods contains Cacti with email only notifications. Second is Nagios XI with email, SMS and Jabber. Basic but in most cases sufficient methods contains Zabbix – email and SMS.

J. *Aditional functions*

The only system which had any additional function was Zabbix with enabled inventory function based on ITIL method.

K. *Cooperation with other systems*

For cooperation with others systems are all compared monitoring system poorly equipped. All of them can provide data directly from database but it must be programmed by custom for specific use.

L. *The depth of monitoring*

All system can check monitor from lower levels up to application state so all of them received one point. All of compared system use SNMP, local agents and standard network protocols.

Table 1 - Point evaluation

Area of evaluation	**Cacti**	**Nagios XI**	**SCOM 2012**	**Zabbix**
Price	3	1	0	3
System requirements	2	1	0	3
User interface	1	2	3	0
Difficulty of implementation	0	2	3	1
Measured load on NIC	1	0	3	2
Reaction to failure	1	2	1	3
Identification of failure segment	1	2	3	1
Automatic search	0	2	3	1
Reporting	1	2	3	2
Additional features	0	0	0	1
Cooperation with another systems	0	0	0	0
Deep of monitoring	1	1	1	1
Total	**11**	**15**	**20**	**18**
Order	**4**	**3**	**1**	**2**

VI. Conclusion

The aim of this paper was to set up the universal comparable methodology and to compare, test and choose suitable monitoring system for smaller network which would also meet all the requirements for supervision of modern ICT environment.

After the first survey and consultations with experts were chosen several suitable candidates from which were finally chosen (after careful consideration of the feasibility of implementation in the laboratory and refused requests about testing versions) four monitoring systems which were used and tested. For these purposes was established methodology of testing and criteria for the selection of the most suitable system. Testing of all chosen monitoring systems was running long-term. Thus it was possible to obtain really relevant data.

At first it is necessary to say, that neither of monitoring systems was absolutely bad. Total loss of Cacti system might seem abysmal but it is probably due to different philosophy to access of network monitoring than in other systems. Unfortunately this system got in the overall evaluation least points.

On the third position is Nagios XI. From the whole paper point of view is this position surprised. From the beginning Nagios XI seems to the author to be professional monitoring system which is able to offer to user everything he needs and something more. The system has a nice and relatively intuitive interface. Overall was its activity also in practical experiences very positive.

Nagios XI on the third position jumped over the freely available monitoring system Zabbix. Zabbix is functionally and parameterised excellent monitoring system. Over the entire period of using the system the author however did not suit up with the subjective logic control and user interface. However, it functionally fulfils everything what a modern ICT environment wants so the second position is in this case well-deserved.

As the best monitoring system from the perspective of this work was chosen commercial product SCOM 2012. The fact that SCOM 2012 won is not in author´s eyes a surprise because who else than operating system vendor himself with offices around the world and with thousands of employees should know how monitoring system should work. Unfortunately a big disadvantage of SCOM 2012 is its price and hardware requirements.

This can be very limiting for most of smaller companies because its implementation could easily climb to hundreds of thousands. However, in terms of functionally is SCOM 2012 absolutely phenomenal and it became well-deserved winner.

VII. References

[1] Cisco Systems, Inc., "Enterprise Campus 3.0 Architecture: Overview and Framework," 2008. [Online]. Available: http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/campover.html. [Accessed 2013 8 13].

[2] J. Case, M. Fedor, M. Schoffstall and J. Davin, "RFC1157: A Simple Network Management Protocol (SNMP)," 5 1990. [Online]. Available: http://www.ietf.org/rfc/rfc1157.txt. [Accessed 6 12 2013].

[3] ZABBIX SIA, "Documentation," 24 5 2012. [Online]. Available: http://www.zabbix.com/documentation.php. [Accessed 12 8 2013].

[4] Nagios Enterprises, LLC, "Nagios - The Industry Standard in IT Infrastructure Monitoring," Nagios Enterprises, LLC, 2013. [Online]. Available: www.nagios.com. [Accessed 13 5 2013].

[5] Microsoft Corporation, "Operations Manager," Microsoft Corporation, 15 1 2013. [Online]. Available: http://technet.microsoft.com/en-us/library/hh205987.aspx. [Accessed 12 8 2013].

[6] O. Mařík, "Analýza dohledových systémů pro datové sítě," 2013. [Online]. Available: http://dspace.upce.cz/bitstream/10195/53944/3/MarikO_Analyza_dohledovych_systemu_pro_datove_site_JH.pdf. [Accessed 1 12 2013].